Notice of Allowability	Application No.	Applicant(s)	
	09/445,385	ZOLOTOREV ET AL.	
	Examiner	Art Unit	
	Thomas M. Ho	2134	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address--

All claims being allowable, PROSECUTION ON THE MERITS IS (OR REMAINS) CLOSED in this application. If not included herewith (or previously mailed), a Notice of Allowance (PTOL-85) or other appropriate communication will be mailed in due course. **THIS NOTICE OF ALLOWABILITY IS NOT A GRANT OF PATENT RIGHTS.** This application is subject to withdrawal from issue at the initiative of the Office or upon petition by the applicant. See 37 CFR 1.313 and MPEP 1308.

1. ☒ This communication is responsive to *8/4/04*.

2. ☒ The allowed claim(s) is/are *1-29*.

3. ☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
   a) ☐ All b) ☐ Some* c) ☐ None of the:
      1. ☒ Certified copies of the priority documents have been received.
      2. ☐ Certified copies of the priority documents have been received in Application No. _____ .
      3. ☐ Copies of the certified copies of the priority documents have been received in this national stage application from the International Bureau (PCT Rule 17.2(a)).

   * Certified copies not received: _____.

Applicant has THREE MONTHS FROM THE "MAILING DATE" of this communication to file a reply complying with the requirements noted below. Failure to timely comply will result in ABANDONMENT of this application.
THIS THREE-MONTH PERIOD IS NOT EXTENDABLE.

4. ☐ A SUBSTITUTE OATH OR DECLARATION must be submitted. Note the attached EXAMINER'S AMENDMENT or NOTICE OF INFORMAL PATENT APPLICATION (PTO-152) which gives reason(s) why the oath or declaration is deficient.

5. ☐ CORRECTED DRAWINGS (as "replacement sheets") must be submitted.
   (a) ☐ including changes required by the Notice of Draftsperson's Patent Drawing Review (PTO-948) attached
      1) ☐ hereto or 2) ☐ to Paper No./Mail Date _____.
   (b) ☐ including changes required by the attached Examiner's Amendment / Comment or in the Office action of Paper No./Mail Date _____.

   Identifying indicia such as the application number (see 37 CFR 1.84(c)) should be written on the drawings in the front (not the back) of each sheet. Replacement sheet(s) should be labeled as such in the header according to 37 CFR 1.121(d).

6. ☐ DEPOSIT OF and/or INFORMATION about the deposit of BIOLOGICAL MATERIAL must be submitted. Note the attached Examiner's comment regarding REQUIREMENT FOR THE DEPOSIT OF BIOLOGICAL MATERIAL.

Attachment(s)

1. ☒ Notice of References Cited (PTO-892)
2. ☐ Notice of Draftperson's Patent Drawing Review (PTO-948)
3. ☒ Information Disclosure Statements (PTO-1449 or PTO/SB/08), Paper No./Mail Date 8/4/04
4. ☐ Examiner's Comment Regarding Requirement for Deposit of Biological Material
5. ☐ Notice of Informal Patent Application (PTO-152)
6. ☐ Interview Summary (PTO-413), Paper No./Mail Date _____ .
7. ☐ Examiner's Amendment/Comment
8. ☒ Examiner's Statement of Reasons for Allowance
9. ☐ Other _____.

Reasons for Allowance

1. The applicant has filed an RCE in response to the Notice of Allowance issued by the Examiner on 5/4/2004. In the RCE, no amendments to the claims were made, however, five additional Information Disclosure Statements were asked to be considered.

2. After a second Examination, the Examiner maintains that even in light of the submitted art of the Information Disclosure Statements, the claims as originally recited are held to be allowable. Nevertheless, some refinements have been made to the reasons for allowance as written in the Ex Parte Quayle action of 8/27/03.

In reference to claim 1, the claim recites the recitation of action of the creation of the blind digital signature "characterized in that during the step of creating the blinded data an RSA-encryption of the chosen initial data is performed". This recitation appears to be missing from the previous reasons for allowance, but it is held to be disclosed by Chaum in the previously cited art 4,759,064. As the cited passage relates to blind digital RSA signatures, it is inherent that the creation of that blind signature, at some point must comprise the RSA encryption process.

Furthermore, in light of the prior art cited by the Applicant, "Provably Secure Blind Signature Schemes" by pointcheval et al. (page 2, 2nd to last, and last paragraph) discloses another digital signature known as a Blind Schnorr Signature in which two large prime numbers p and q are

chosen and published with an element g of (Z/pZ), otherwise known as a Ring structure in abstract algebra. This relationship is held to be equivalent to two numbers g and p being coprime as an essential property of coprime numbers.

Furthermore, the Blind Schnorr scheme calls for the creation of a pair of keys such that $X \in Z/qZ$ and $y = g^{-x} \bmod p$.

This scheme appears to disclose the additional masking factor g coprime to large prime number p. However, this prime number is not an exponent, nor does the Schnorr blind digital signature scheme expressly call for the use of RSA as its encryption scheme. No art of record or found discloses the coprime masking factor to each admissible public RSA exponent in addition to the other reasons for allowance have been found, nor is there any motivation to combine, and the reasons for allowance remain substantially the same as set forth in the action of 8/27/03.

Accordingly, the claims are held to be allowable.

Conclusion

3. Any inquiry concerning this communication from the examiner should be directed to Thomas M Ho whose telephone number is (571)272-3835. The examiner can normally be reached on M-F from 9:30 AM - 6:00 PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gregory A. Morse can be reached on (571)272-3838.

The Examiner may also be reached through email through Thomas.Ho6@uspto.gov

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is (571)272-2100.

General Information/Receptionist	Telephone: 571-272-2100	Fax: 703-872-9306
Customer Service Representative	Telephone: 571-272-2100	Fax: 703-872-9306

TMH

September 4th, 2005

GREGORY MORSE
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100